Statement by Mr. Scott Kriens
Chairman and CEO
Juniper Networks, Inc.
Before the Committee on Government Reform

May 11, 2006

Mr. Chairman, Congressman Waxman, members of the Committee. It is a great pleasure to testify here today about continuity of operations in the event of a serious pandemic.

A mutation of the much publicized bird or avian flu virus, one that precipitates and accelerates human-to-human transmission, is almost unimaginable to most of us here. Over crowded hospitals, quarantined communities, millions of lives at risk, our national economy crippled, stand in sharp contrast to the comforts of this room, our homes and our workplaces today.

Of course, one year ago who among us could have imagined New Orleans under water just a few months later? Five years ago, no one imagined human beings would actually hijack commercial aircraft and deliberately crash them into the World Trade Center or the Pentagon. The tsunami in Indonesia, bombings in the United Kingdom and Spain, a world at war, and the United States as the world's only superpower, stands at center stage both for its own domestic crises and for world crises as well.

In light of these catastrophes, Americans recognize the importance of emergency preparedness by the U.S. government, the private sector, and individuals, in times of national crisis. Being prepared translates into the ability of essential employees to communicate and execute their responsibilities 24/7 anywhere, anytime. This capability is known as continuity of operations or COOP. When working with our enterprise customers to prepare for such a "perfect storm" scenario, we at Juniper Networks believe in insuring they have a secure and resilient infrastructure. The cornerstone of this round-the-clock COOP capability is a technically robust and cost-effective telework system that can deliver instant, highly secure access to every remote user – where and when they need it.

Telework, or remote work, is a concept that has gained much attention as a means for improving the productivity of the workforce while addressing pressing environmental and transportation challenges for American society. In the commercial world, private sector companies have been taking advantage of telework for years. Business managers realize that telework is a way to get optimal performance from their workers, allowing employees to get work done from home or the road, providing the operational flexibility that our modern economy demands. I find it ironic that many government managers reportedly equate telework with reduced employee work hours and lower productivity,

believing in the outdated management philosophy that "if I can't see you, I can't manage you." Business sees it the other way around, as a means of maximizing worker productivity, with the added benefits of lower commuting costs and improved quality of life as motivators and morale-builders.

Beyond these issues of day-to-day telework applications, it is our task in the context of today's hearing to concentrate on the critical linkage between telework and national security, and to provide the most effective telework capability for COOP given limited resources. It is worth noting that the internet was first conceived and created by the Defense Advanced Research Projects Agency (DARPA) as a means for sending information over a skeleton communications system in the case of a nuclear war. So from its genesis, the internet was envisioned as a communications system to support COOP in a national emergency. Today the internet is a pillar of our national economy and government operations at all levels. Executive branch agencies need only take technologies and management practices that are readily available and bring them to bear on this task to ensure that essential personnel can perform their vital duties in the case of a pandemic or other national crisis.

The Executive Branch agencies are not alone in needing to enhance their remote work plans for COOP. My bet is that Congress could benefit from an improved remote work plan, as could state and local government and American industry. There is no question that all of us can and must do a better job of COOP planning generally, but remote work planning especially.

At Juniper Networks, telework is not only a critical component of how we work as a company, but also how we think about our customers and develop our products. I offer this Committee four recommendations that I hope will prove helpful as you consider how the government needs to prepare for a potential pandemic.

1. TECHNOLOGY IS AVAILABLE TODAY - FOR EFFECTIVE CONTINUITY OF OPERATIONS THROUGH TELEWORK

We are all personally familiar with the connectivity to the workplace the Internet affords us. It has changed our lives. With email and web access, we are able to log on and accomplish work from out of the office that we would never have dreamed of until a few years ago. Achieving the connectivity and control that is necessary to maintain government operations in a crisis, however, offers a much more technically demanding set of requirements than simply surfing the web. Cutting edge technology enables us to meet these requirements. With the hardware and software currently on the market, we can create a network of remote users who, using phone, internet, and an array of collaborative tools could continue to execute essential government operations from remote locations.

What are the requirements we must meet to establish an effective remote work system for COOP? At the most basic level, there are two.

First, there needs to be an integrated and intelligent infrastructure that provides for the ready transmission of data, through close "integration" of all the components of the system and the right "intelligence" to help make this happen. The teleworking infrastructure is most likely the same one we use on a daily basis to communicate from our homes, consisting of the wires, fiber, and transmission towers that we all rely upon. For more challenging scenarios, however, emergency communications systems that rely on satellite communications may be required. Data flow is the essential requirement, and whether it moves through wires, fiber, or the air, it will have to be robust enough to function through a crisis.

The second requirement is network security--guaranteeing end-to-end security across the teleworking infrastructure as that remote user is gaining access to critical resources.

For example, a telework system for COOP will require virtually 100 percent confidence that the system can remotely authenticate who is accessing and using what information, and ensure that they access and use only information for which they have authorization.

Users must be able to access files securely and share information from a headquarters location anywhere, anytime, on multiple products operating on multiple platforms. The system must provide high confidence that computing technologies it uses also are authenticated as to their "trustworthiness" vis-à-vis viruses or other security breaches.

The products needed to establish and maintain just such a secure system are available now, waiting on the shelf for deployment. So the question is not whether we can establish a trusted and secure teleworking environment to support COOP, but rather how and when the system is put in place.

2. FOCUS ON CRITICAL EMPLOYEES

In our view, the best place to launch an effective telework implementation for COOP is to start with our Nation's leaders, senior and critical executives. These are the individuals who must be able to plan, organize, and execute their agencies responses in disaster or emergency situations. Their ability to work is essential. They will set the example for how their agencies will be able to expand remote work to all of their employees to maintain operations in emergencies. Moreover, a successful COOP system will demonstrate the viability of remote work for telework during day-to-day operations as well.

The equipment and installation costs for establishing the COOP system will not bust agency budgets. The functionality the system would provide is well worth the investment in terms of the capability for COOP the system will provide. Perhaps the most challenging aspect of making the remote work system effective is putting policies and procedures in place that support orderly operations and that complement the ability of today's technologies to allow secure, auditable information sharing. While this is a challenge, it is crucial for the system's success, and therefore worth the effort.

I think it is important not to focus this effort solely on Executive Agencies, but on Congress as well. You as Members, and Congress as an institution, should write a plan and establish a remote work system. Putting a system in place and conducting, say, quarterly exercises yourselves and with your key staff would make the plan operational and allow you to identify and implement improvements to the business rules and technical environments that make it work. If you had possessed such a system back in 2001 during the anthrax attacks, when the House office buildings were shut for over a week, and the Senate Hart Building was closed for over three months, it would have made an enormous difference to your ability to continue your vital work.

Imagine if this were done among essential employees across the Federal government as well. I believe the result would be improved preparedness certainly, but more importantly, I believe local and state jurisdictions and American industry would better appreciate the problem and would follow the Federal lead.

3. MAINTAIN THE INTEGRITY OF THE NETWORK–BY AUTHENTICATING AND AUTHORIZING END USERS

Effective remote work plans have two significant components: business rules to determine who has access to what information and under what conditions, and the technical environment that supports the business rules. It is the technical environment that constitutes Juniper's expertise and it is my intention to show you that information can be securely and effectively managed and tracked from multiple remote locations by any number of authorized users. The key is to have qualified guards at the gates of your critical information, guards that authenticate those seeking access and the equipment they are using to gain that access. These "guards" are technologies that easily reside on your network and navigate user and equipment access according to rules set by the governing organization. We call this comprehensive "network policing" of end user/equipment Unified Access Control.

Just a few years ago, the security of information could only be secured by equipping computers with software and component hardware that required expensive and routine maintenance and upgrade. Today, your network can function as the guard at the gate, performing that same function, more effectively,

at lower cost and with greater ease for the user. Access and information management protocols are set within the network in accordance with the business rules that are established. The network will determine whether your home PC, hotel business center or other access tool meets network standards to access information resources. And remember, unified access control ensures that the individual seeking access also is authorized.

The bottom line is that today, through your network, you can authenticate the user seeking access to ensure appropriate authorization and the equipment being used to protect against viruses, intrusions and other breaches.

4. OPEN STANDARDS ALLOW USE OF BEST-OF-BREED TECHNOLOGIES AND LOWER COSTS

In an emergency, communications necessarily will come from many sources. Technologies that govern information access and authentication must be able to recognize and interoperate with a spectrum of these technologies. The governing technologies themselves should be as interoperable as practicable with technologies from any number of manufacturers. This not only allows implementation of the best-of-breed solutions and increases operational efficiency, but also leads to lower operating cost.

CONCLUSION

To summarize, "top down" remote or telework planning and execution is critical for dealing with the grave impacts of a national crisis like an avian flu outbreak. We must get our Nation where we need to be in terms of a 24/7 essential employee, work anywhere, capability. We, as a country can be prepared for this impending perfect storm, by working together to ensure a secure and resilient infrastructure is in place and ready throughout our government; and we can start right here. The ability to effectively manage information and authorize and authenticate remote users *and* their equipment is both possible and practical today.

The President's Implementation Plan for the National Strategy for Pandemic Influenza speaks to the need to improve telework capability to maintain COOP during a pandemic. It specifically requires the Office of Personnel Management to update its key telework management documents to include guidance for how best to use telework in support of COOP. I recommend that to the extent possible, this guidance focus on applying telework practices and procedures used by agencies on a daily basis to support the special circumstances of a pandemic outbreak or other emergency. A specialized telework system that is used only during an emergency will run a higher risk of problems and failures than a system that is familiar to the workforce through use on a daily or weekly basis.

Finally and just as importantly, an added benefit of "top down" remote work planning is that expansion of telework, and hence the broader benefits referenced earlier, are more likely and achievable when senior management experiences firsthand the processes involved. The United States then gains not only critical COOP advantages, but also the potential for the most advanced 21st century workforce anywhere.

I look forward to assisting the Committee in every possible way as you move forward. I would be pleased to answer any questions you might have.

On behalf of Juniper Networks, thank you for the opportunity to speak before you today. I look forward to answering your questions.

Contact:
MacKenzie Ruggiero
Juniper Networks
mruggiero@juniper.net
571-203-1987